



Privacy Policy

Version 1.0.0 · Last updated 2026-04-16 · liivra.com/legal/privacy-policy

Liivra (Pty) Ltd ("**Liivra**", "**we**", "**us**", or "**our**") is committed to protecting your personal information in accordance with the Protection of Personal Information Act 4 of 2013 ("**POPIA**") and all other applicable South African legislation. This Privacy Policy explains what personal information we collect, why we collect it, how we use and protect it, and what rights you have.

By using the Liivra mobile application, website at liivra.com (<https://liivra.com>), or any related services (collectively, the "**Platform**"), you acknowledge that you have read and understood this Privacy Policy.

1. Information Officer

Our designated **Information Officer** is responsible for ensuring compliance with POPIA and for handling all data-related queries:

- **Name:** Therry Martins
- **Email:** privacy@liivra.com
- **Phone:** +27 78 716 0366
- **Postal address:** 20 Mirage Drive, Helderkruijn, Gauteng, South Africa 1724

You may contact the Information Officer at any time regarding questions about this Privacy Policy or to exercise your rights under POPIA.

2. Personal Information We Collect

We collect different categories of personal information depending on how you interact with the Platform and your role (Tenant, Buyer, Landlord, Seller, Agent, or Visitor).

2.1 Information you provide directly

| Category | Examples | |---|---| | **Identity information** | Full name, South African ID number or passport number (for KYC verification), date of birth, gender | | **Contact information** | Email address, phone number, physical address | | **Account credentials** | Email/password or social sign-in tokens (Google, Apple) | | **Profile information** | Profile photo, role selection, preferred language, home city | | **Financial information** | Bank account details (for payouts), payment method selections, transaction history through Liivra Pay | | **Listing content** | Property descriptions, photographs, 360-degree virtual tour media, 3D dollhouse scans, floor plans, pricing, availability | | **Application data** | Rental or purchase applications, supporting documents (proof of income, employment letters, credit references) | | **Communication data** | Messages sent through in-app chat, enquiry forms, support tickets | | **KYC / biometric data** | Selfie photographs for liveness verification, ID document images submitted to our verification partner |

2.2 Information collected automatically

| Category | Examples | |---|---| | **Device information** | Device model, operating system, app version, unique device identifiers, push notification tokens | | **Usage data** | Pages and screens viewed, search queries, filters applied, listings saved or shared, time spent on listings, feature interactions | | **Location data** | Approximate location derived from IP address; precise GPS location only when you explicitly grant permission for location-based property search | | **Log data** | IP address, browser type (web), access times, referring URLs, crash reports |

2.3 Information from third parties

| Source | Information | |---|---| | **Smile Identity** (KYC provider) | Identity verification results, document authenticity scores, liveness check outcomes | | **Payment processors** (Paystack, Ozow, Stitch Pay) | Transaction status, payment confirmations, refund status | | **Firebase Authentication** | Social login profile data (name, email, profile photo) when you sign in via Google or Apple |

3. How We Use Your Personal Information

We process your personal information for the following purposes:

1. **Account management** — Creating, maintaining, and securing your account.
2. **Property matching and search** — Displaying relevant listings based on your preferences, search history, location, and budget.
3. **AI-powered recommendations** — Our AI algorithms analyse your search patterns, saved listings, and stated preferences to suggest properties you may be interested in. See Section 4 for details.
4. **AI-powered valuations** — Generating estimated property values based on market data, comparable sales, location factors, and listing attributes. See Section 4 for details.
5. **Escrow and payment processing** — Facilitating Liivra Pay trust account transactions, holding deposits, processing rental payments, and managing fund releases.
6. **Identity verification** — Verifying your identity through our KYC partner to prevent fraud and comply with the Financial Intelligence Centre Act 38 of 2001 ("**FIC Act**").
7. **Communications** — Sending transactional notifications (application updates, payment confirmations, tour reminders), responding to support requests, and delivering service announcements.
8. **Analytics and improvement** — Understanding how users interact with the Platform to improve features, fix bugs, and enhance the user experience.
9. **Fraud prevention and safety** — Detecting and preventing fraudulent listings, fake accounts, and abusive behaviour.
10. **Legal compliance** — Meeting our obligations under POPIA, the FIC Act, the Tax Administration Act 28 of 2011, the Companies Act 71 of 2008, and other applicable laws.
11. **Marketing** — With your opt-in consent, sending promotional communications about new features, listings in your area, or platform updates. You may opt out at any time.
12. **Dispute resolution** — Investigating and resolving complaints, disputes, and Liivra Pay transaction issues.

4. AI Features and Your Data

Liivra uses artificial intelligence in several features. We believe in transparency about how AI interacts with your personal information.

4.1 AI property matching

Our matching algorithm considers your stated preferences (location, budget, property type, number of bedrooms), your search and browsing history on the Platform, and properties you have saved or enquired about. The algorithm generates a personalised relevance score for each listing. **No human reviews individual matching decisions**, but you can always browse all listings manually.

4.2 AI price estimates

Liivra generates estimated market values for properties using machine-learning models trained on publicly available property transaction data, municipal valuations, and listing attributes (size, location, condition, amenities). **AI price estimates are not professional property appraisals, sworn valuations, or financial advice.** They are indicative estimates that may be inaccurate. You should not rely solely on an AI estimate when making purchasing, selling, or rental decisions. We recommend obtaining an independent professional valuation.

4.3 AI content moderation

We use automated tools to screen listing descriptions and images for prohibited content (discriminatory language, misleading claims, inappropriate imagery). Flagged content is reviewed by a human moderator before removal.

4.4 Your choices

You may request information about the logic involved in any automated decision that significantly affects you, and you may request human intervention, by contacting privacy@liivra.com.

5. Legal Bases for Processing

Under POPIA, we process personal information based on one or more of the following legal grounds:

| Legal basis | When it applies | |---|---| | **Consent** (POPIA s11(1)(a)) | Marketing communications, optional location sharing, optional analytics | | **Contract** (POPIA s11(1)(b)) | Account creation, listing publication, escrow transactions, application processing | | **Legal obligation** (POPIA s11(1)(c)) | KYC/AML compliance under the FIC Act, financial record-keeping under the Tax Administration Act, data breach notification | | **Legitimate interest** (POPIA s11(1)(f)) | Fraud prevention, platform security, service improvement, AI-powered recommendations (balanced against your rights) |

6. Sharing Your Personal Information

We do not sell your personal information. We share it only with the following categories of recipients, and only to the extent necessary:

6.1 Other users

- **Landlords and Agents** see your name, contact details, and application documents when you submit an enquiry or rental/purchase application.
- **Tenants and Buyers** see listing details, agent contact information, and landlord/seller identity where applicable.
- **You control** what you share through your profile visibility settings.

6.2 Service providers

| Provider | Purpose | Data shared | |---|---|---| | **Supabase** (database hosting) | Storing listings, applications, user profiles, transaction records | Account data, listing data, application data | | **Firestore** (Google) | Authentication, push notifications, crash reporting, analytics, chat, media storage | Auth tokens, device tokens, crash logs, chat messages, images, 360-degree media | | **Paystack** | Payment processing | Transaction amounts, payment method tokens | | **Ozow** | EFT payment processing | Transaction amounts, bank references | | **Stitch Pay** | Account-to-account payments | Transaction amounts, account references | | **NOWPayments** | Cryptocurrency payments (where available) | Transaction amounts, wallet references | | **Smile Identity** | Identity verification (KYC) | ID document images, selfie images, name, ID number | | **PostHog** | Product analytics | Anonymised usage events, device type, feature interactions | | **Sentry** | Error monitoring | Crash reports, device info, anonymised user IDs | | **Resend** | Transactional email delivery | Email address, email content | | **Microsoft Clarity** | Session heatmaps (web only) | Anonymised click/scroll behaviour |

All service providers are bound by data processing agreements ("DPAs") that require them to process your data only on our instructions and to maintain appropriate security measures.

6.3 Legal and regulatory

We may disclose personal information where required by law, court order, subpoena, or regulatory request, including to the South African Revenue Service, the Financial Intelligence Centre, or the Information Regulator.

6.4 Business transfers

In the event of a merger, acquisition, or sale of all or part of our business, your personal information may be transferred to the acquiring entity, subject to the same privacy protections.

7. International Data Transfers

Your personal information may be processed and stored outside South Africa:

- **Google Cloud Platform** (Firestore, Cloud Run): Data may be processed in the United States (us-east1 region) and other Google data-centre locations.
- **Supabase**: Hosted on AWS infrastructure; data centre location is configured per project.
- **PostHog**: Cloud-hosted analytics with data processing in the United States and European Union.
- **Sentry**: Error data processed in the United States.

Where personal information is transferred outside South Africa, we ensure that adequate safeguards are in place, including:

- Transfers to countries with adequate data protection laws as recognised by the Information Regulator.
- Standard contractual clauses or binding corporate rules with service providers.
- Your explicit consent where required.

This is in compliance with POPIA s72, which permits cross-border transfers where the recipient is subject to comparable privacy laws or binding agreements.

8. Data Retention

We retain your personal information only for as long as necessary to fulfil the purposes described in this Privacy Policy, or as required by law:

| Data category | Retention period | Legal basis | |---|---|---| | **Account data** (profile, preferences) | Life of account + 5 years after account deletion | Companies Act s24 (record-keeping) | | **Financial and transaction records** | 7 years from date of transaction | Tax Administration Act s29; FIC Act | | **KYC documents** (ID images, selfies, verification results) | 5 years from the date of last transaction or account closure | FIC Act s22 | | **Chat messages** | Life of account + 1 year after account deletion | Contractual necessity | | **Analytics data** | Aggregated and anonymised after 24 months | Legitimate interest | | **Crash reports and logs** | 90 days | Legitimate interest (debugging) | | **Marketing consent records** | Duration of consent + 1 year after withdrawal | POPIA compliance (proof of consent) |

After the applicable retention period, personal information is permanently deleted or irreversibly anonymised.

9. Data Security

We implement appropriate technical and organisational measures to protect your personal information against unauthorised access, loss, destruction, or alteration:

- **Encryption in transit:** All data transmitted between your device and our servers uses TLS 1.2 or higher.
- **Encryption at rest:** Databases and file storage are encrypted using AES-256 or equivalent.
- **Access controls:** Role-based access with the principle of least privilege. Multi-factor authentication for internal systems.
- **Audit logging:** All access to personal information is logged and monitored.
- **Incident response:** We maintain a data breach response plan with notification procedures as required by POPIA s22.
- **Regular reviews:** Security practices are reviewed and updated at least annually.

No system is completely secure. While we take all reasonable steps to protect your data, we cannot guarantee absolute security.

10. Your Rights Under POPIA

As a data subject, you have the following rights under POPIA sections 23 to 25:

1. **Right of access** (s23) — You may request confirmation of whether we hold personal information about you and request a copy of that information.
2. **Right to correction** (s24) — You may request that we correct or update inaccurate, incomplete, or misleading personal information.
3. **Right to deletion** (s24) — You may request that we delete your personal information where it is no longer necessary for the purpose it was collected, subject to legal retention requirements.
4. **Right to object** (s11(3)) — You may object to the processing of your personal information on grounds of legitimate interest, or object to receiving direct marketing.
5. **Right to data portability** — You may request your personal information in a structured, commonly used, machine-readable format.
6. **Right to withdraw consent** — Where processing is based on consent, you may withdraw that consent at any time without affecting the lawfulness of processing before withdrawal.
7. **Right not to be subject to automated decisions** (s71) — You may request human intervention in any automated decision that significantly affects you.

How to exercise your rights

- **In-app:** Navigate to Profile ' Settings ' Privacy & Data.
- **Email:** Send a request to privacy@liivra.com with the subject line "POPIA Data Request".
- **Postal:** Write to our Information Officer at the address listed in Section 1.

We will respond to your request within 30 days. We may need to verify your identity before processing your request. If we cannot comply with a request, we will provide reasons in writing.

11. Cookies and Tracking Technologies

The Liivra mobile application does not use browser cookies. However, our website at liivra.com (<https://liivra.com>) uses cookies and similar technologies. For full details, please see our Cookie Policy (/legal/cookie_policy).

In the mobile app, we use:

- **Firebase Analytics** for anonymised usage analytics.
- **PostHog** for product analytics and feature-flag evaluation.
- **Sentry** for crash and error reporting.
- **Push notification tokens** (Firebase Cloud Messaging) for delivering notifications you have opted into.

You can manage analytics preferences in Profile ' Settings ' Privacy & Data ' Analytics Preferences.

12. Children's Privacy

The Platform is not intended for use by persons under the age of 18. We do not knowingly collect personal information from children under 18. If you are under 18, you may only use the Platform with the involvement and consent of a parent or legal guardian.

If we become aware that we have collected personal information from a child without appropriate guardian consent, we will take steps to delete that information promptly. If you believe a child has provided us with personal information, please contact privacy@liivra.com.

13. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or business operations. When we make material changes:

- We will update the "Last updated" date and version number at the top of this document.
- We will notify you via email (to the address associated with your account) and through an in-app notification.
- Where required by law, we will obtain your consent to material changes before they take effect.

We encourage you to review this Privacy Policy periodically.

14. Contact Us

If you have any questions, concerns, or complaints about this Privacy Policy or our data practices:

- **Email:** privacy@livra.com
- **General support:** support@livra.com
- **Postal:** [Registered office address — to be confirmed]

If you are not satisfied with our response, you have the right to lodge a complaint with the **Information Regulator (South Africa)**:

- **Johannesburg:** JD House, 27 Stiemens Street, Braamfontein, 2001
- **Phone:** 010 023 5207
- **Email:** inforeg@justice.gov.za
- **Website:** <https://inforegulator.org.za> (<https://inforegulator.org.za>)